NATIONAL INSTITUTE OF TECHNOLOGY PATNA
Department of Computer Science & Engineering
MID SEMESTER EXAMINATION, January - July 2022

B. Tech: Semester-VI

Course Name: Information Security **Code: CS6404**

Maximum Time: 2 hours **Max. Marks: 30**

Instruction:

1. Attempt All questions (Only Question number 7 does not have any alternative).
2. Assume any suitable data, if necessary.
3. The Marks, CO (Course Outcome) and BL (Bloom's Level) related to questions are mentioned on the right-hand side margin.

		Marks	**CO**	**BL**
1.a.	Online banking and automated clearing house (ACH) transfers were used extensively by a small family-owned construction company. Employees used both a company and a user-specific ID and password to log in. An ACH transfer of $10,000 was initiated by an unknown source, according to the owner. They contacted the bank and discovered that cyber crooks had made six $550,000 payments from the company's bank accounts in only one week. One of their employees had opened an email from a materials supplier that turned out to be a malicious email loaded with a keylogger sent from an imposter account. Classify the type of attack it was. Give justification to support your answer.	5+5	CO1, CO3	A
b.	The CEO of a government contracting firm was alerted that access to their company's commercial data, including their military client database, was being sold in a dark web auction. The CEO quickly realized that the information being sold was outdated and unrelated to any government agency clients. The company discovered that a senior employee had unknowingly downloaded a malicious email attachment from a trustworthy source. Identify the affected information security principals. Give justification to support your answer.			
OR				
2.a.	Define and differentiate between threat, vulnerability, and risk with an example.	5	CO3	R, U
b.	Enumerate important defense considerations against active and passive attacks.	5		
3.	'FreeChat,' a new social networking platform, debuted in September 2021. The majority of its users are between the ages of 13 and 21. Users can: share photographs and status updates; send private messages; play games with other users; and make in-app purchases. Their headquarters are in Patna, and they have a staff of 50 individuals. All employees have a staff permit that allows them to enter the facility, as well as a business iPhone and laptop. Although all employees received an email explaining	10	CO2	E, C

<table>
<tr><td></td><td>best practices for cyber security, not everyone read it, and no mandatory training on information security was provided.

Generate a report in below tabular format by identifying their Informational assets, potential security threats to those assets and also prescribe security mechanisms for mitigating those threats.

<table><tr><td>Informational assets</td><td>Potential cyber security threats to assets</td><td>Security mechanisms</td></tr><tr><td></td><td></td><td></td></tr></table></td><td></td><td></td><td></td></tr>
<tr><td colspan="5">OR</td></tr>
<tr><td>4.</td><td>Articulate a detailed information security policy for 'FreeChat’, also recommend different standards and laws the company must compile with.</td><td></td><td>CO 2</td><td>E, C</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>5.</td><td>Encrypt your name (as plaintext) using the Caesar Cipher. The secret key you will use is the <i>last 3 digits of your roll number mod 26</i>. Find the vulnerability of the cipher. Identify the attack to which the cipher is vulnerable. Discuss that attack.</td><td>5+2+1+2</td><td>CO4</td><td>P</td></tr>
</table>

End of Questions

Level	Bloom's Taxonomy
1	Remembering (R)
2	Understanding (U)
3	Applying (P)
4	Analyzing (A)
5	Evaluate (E)
6	Create (C)

Course Outcomes:

At the end of the course, a student should have:

CO	Outcome
1.	Identify the appropriate technologies necessary to solve concrete problems related to confidentiality (cryptographic solutions), integrity (authentication such as biometric), availability (for example, intrusion detection solutions), and privacy protection.
2.	Develop policies and procedures to manage enterprise security risks.

3.	Evaluate and communicate the human role in security systems with an emphasis on ethics, vulnerabilities and training.
4.	Apply cryptography and some key encryption techniques for providing secure solutions
5.	Determine appropriate mechanisms for protecting information systems ranging from operating systems to database management systems and to applications.